OMB Approval 2700-0042

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

1. CONTRACT ID CODE	PAGE	OF	PAGE(S)
	1		2

2. AMENDMENT/MODIFICATION NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO. *(If applicable)*
1	See Block 16C	N/A	

6. ISSUED BY CODE

National Aeronautics and Space Administration
Langley Research Center
Hampton, VA 23681-2199

7. ADMINISTERED BY *(If other than Item 6)* CODE

8. NAME AND ADDRESS OF CONTRACTOR *(No. Street, County, State and ZIP: Code)*

ARINC Engineering Services, LLC
2551 Riva Road
Annapolis MD 21401-7435

CODE FACILITY CODE

(4)	9A. AMENDMENT OF SOLICITATION NO.
	9B. DATED *(SEE ITEM 11)*
X	10A. MODIFICATION OF CONTRACT/ORDER NO. NNL06AA03B
	10B. DATED *(SEE ITEM 13)* January 13, 2006

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

☐ The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers ☐ is extended, ☐ is not extended.

Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods: (a) By completing Items 8 and 15, and returning one (1) copy of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATA SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and data specified.

12. ACCOUNTING AND APPROPRIATION DATA *(If required)*

N/A

13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/ORDERS, IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

(4)	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: *(Specify authority)* THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.
	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES *(such as changes in paying office, appropriation date, etc.)* SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).
	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:
X	D. OTHER Specify type of modification and authority) Mutual Agreement

E. IMPORTANT: Contractor ☐ is not, ☒ is required to sign this document and return ___1___ copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION *(Organized by UCF section headings, including solicitation/contract subject matter where feasible.)*

The purposes of this modification are to add or delete several FAR/NFS clauses and to incorporate Exhibit E (IT Security Implementation Plan).

(continued on next page.)

Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER *(Type or print)*	16A. NAME AND TITLE OF CONTRACTING OFFICER *(Type or print)*
Mario F Martin PE	C. LYNN JENKINS

15B. CONTRACTOR/OFFEROR	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA	16C. DATE SIGNED
(Signature of person authorized to sign)	6 Jun 06	BY *(Signature of Contracting Officer)*	6-6-06

1. Section I (Contract Clause), Paragraph I.1 (LISTING OF CLAUSES INCORPORATED BY REFERENCE): The following clauses are hereby added or deleted in their entirety as follows:

   ADDED because it "is" applicable for use in cost reimbursable contracts:

   "FAR 52.243-2 APR 1984 Changes – Cost-Reimbursement (Alternate V)"

   ADDED because of potential use under this contract:

   "NFS 1852.245-76 OCT 1988 List of Government-Furnished Property"

   DELETED because it "is not" applicable for use in cost reimbursable contracts:

   "FAR 52.245-19 APR 1984 GOVERNMENT PROPERTY FURNISHED "AS IS""

2. Section J (LIST OF ATTACHMENTS), Paragraph J.1 (CONTRACT DOCUMENTATION REQUIREMENTS), Exhibit E (IT Security Implementation Plan): The Contractor's IT Security Implementation Plan submitted via email on February 13, 2006 and as accepted by the LaRC Information Technology Security Manager (ITSM) on April 6, 2006 has been approved and is hereby incorporated as Exhibit E to this contract.

3. All other terms and conditions remain unchanged.

NNL06AA03B

IT SECURITY IMPLEMENTATION PLAN

1. PURPOSE

The purpose of this plan is to document the implementation plan for IT Security for the ARINC team activities on the NASA Flight Critical Systems Research (FCSR) contract, NNL06AA62T. This plan applies to unclassified information technology (IT) systems and networks under NASA's purview operated by or on behalf of the Federal Government.

1.1 Policy

Requirements for IT security have been embodied in the Public Laws of the United States or promulgated by other directives of the Federal Government. All organizations which process Government information, regardless of whether they are Federal or contractor entities, are responsible for the following:

a. Participating in an IT Security Program (PL 100-235 and OMB Circular A-130).
b. Protecting personal information contained in a system of records (Pub. L 93-579, as amended).
c. Certification (or authorization) of major applications (OMB Circular A-130).
d. Assessment, analysis, and management of risks (OMB Circular A-130).
e. Personnel screening for IT access (OMB Circular A-130).
f. IT security awareness and training (PL 100-235 and OMB Circular A-130).
g. Response to and reporting of IT security incidents (OMB Circular A-130).

ARINC's Information Systems Security Program ensures networked information resources and systems are secure by reducing the risk of compromise to an acceptable level, assuring operational continuity of information systems, and maintaining the integrity of ARINC's corporate information.

ARINC prohibits unauthorized access, disclosure, duplication, modification, diversion, or destruction of, as well as the loss, misuse, or theft of corporate information. Users shall report all incidents that breach the Information Systems Security Policies to the Information Systems Security Representative in their respective division or organization.

Classified systems shall adhere to the appropriate classified policy documents. All proposals that involve existing, projected or proposed network systems shall adhere to the Information Systems Security Policies.

ARINC Information Systems Security Policies and the mechanisms and products subject to those policies shall be reviewed annually and updated when necessary to ensure that the following objectives continue to be satisfied. This annual review shall be completed by the Information Systems Security Manager and shall, as a minimum, cover the below elements.

- Reduction of risk
- Continuity of operations
- Integrity of information
- Confidentiality of information
- Compliance with applicable laws

1.2 Goals and Objectives

The goal of this IT security implementation plan is to ensure compliance with the security requirements outlined in NASA Policy Directive (NPD) 2810.1, Security of Information Technology, and NASA Procedures and Guidelines (NPG) 2810.1, Security of Information Technology. This includes compliance with the following Federal directives and guidelines that deal with IT Security, as they apply to Government contractors:

a. OMB Circular A-130, Management of Federal Information Resources
b. OMB Circular A-130 Appendix III, Security of Federal Automated Information Resources
c. Computer Security Act of 1987
d. Applicable Federal Information Processing Standards (FIPS).

The ARINC FCSR Program Manager shall ensure that all systems connected to a NASA network or operated by ARINC for NASA conform with NASA and Center security policies and procedures. The security measures and program safeguards to ensure that IT resources:

- Are protected from unauthorized access, alteration, disclosure, or misuse of information processed, stored, or transmitted
- Can maintain the continuity of automated information support for NASA programs and functions
- Incorporate management, general, and application controls sufficient to provide cost-effective assurance of the systems' integrity and accuracy
- Have appropriate technical, personnel, administrative, environmental, and access safeguards
- Document and follow a virus protection program for all IT resources under its control
- Document and follow a network intrusion prevention program for all IT resources under its control.

1.3 Assignment of Responsibility

The Contract will organizationally be a part of ARINC Engineering Services, LLC. The FCSR program and ARINC corporate responsibilities for IT Security are delineated in the following subsections.

1.3.1 Program Manager

The FCSR Program Manager, with support from ARINC's corporate Network Services Director are responsible for the implementation of this plan, as approved by the NASA CO, for all FCSR activities undertaken by the ARINC team.

1.3.2 ARINC FCSR Information Systems Security Representative

The FCSR Program Manager shall designate an Information Systems Security Representative to champion, facilitate, and coordinate Information Systems Security initiatives and issues for the FCSR tasks. The representative shall undergo sufficient training and procure the supporting materials and other resources necessary to properly perform this function.

1. The Information Systems Security Representative shall advise program and task management on compliance with IT Security policies

2. Establish Program procedures necessary to comply with the Information Systems Security Policies
3. Provide direction for changing technology
4. Ensure Program compliance with Information Systems Security Policies
5. Specifically assign responsibilities for control measures to protect information assets
6. Allocate resources and staff attention to address Information Systems Security
7. Ensure that users are briefed on the Information Systems Security Policies and their respective responsibilities relative to those policies
8. Ensure that users are provided with training and supporting reference materials needed to properly protect project information
9. Provide technical resources to ensure that solutions for complying with the Information Systems Security Program are complete.

1.3.3 Infrastructure Control Board Management (ICBM)

The ICBM provides strategic direction for ARINC's Information Systems Security Program, and has designated and authorized the Enterprise Configuration Control Board (ECCB) to carry out the directive functions of the ARINC Information Systems Security Program.

1.3.4 Information Systems Security Manager (ISSM)

The ISSM originates and recommends for approval activities, projects and policies necessary to maintain ARINC's responsive and effective Information Systems Security Program. The ISSM shall:

1. Originate and recommend for approval the Information Systems Security Policies.
2. Develop, maintain and interpret the Information Systems Security Policies
3. Provide training and information on Information Systems Security within ARINC
4. In association with division representatives, develop or assist in developing Business Unit-specific procedures that implement and support the Information Systems Security Policies.
5. Coordinate implementation of Information Systems Security controls and mechanisms.
6. Coordinate risk assessments for Information Systems Security waiver and deviation requests for Business Units.
7. Establish an on-going awareness program to regularly remind Users of the importance of Information Systems Security for ARINC and of each person's obligations with respect to Information Systems Security.
8. Identify and publicize sufficient training and supporting reference materials to allow all Users to properly protect corporate information. Investigate security incidents; recommend steps to minimize ARINC exposure to such threats.

1.3.5 Enterprise Configuration Control Board (ECCB)

The ECCB will review and respond to all ARINC audits, incidents, and waiver and change requests. Additionally, the ECCB shall provide the ICBM with compliance status as requested. For matters pertaining to Information Systems Security, the ECCB reports directly to the ICBM and shall be comprised of at least one member from each of the following ARINC divisions and business units. Other representatives may be invited to participate in ECCB meetings as required. The ECCB shall:

1. Forward new or modified Information Systems Security Policies to the ICBM

2. Ensure that Information Systems Security is integrated with other ARINC planning processes
3. Provide status and approval/disapproval recommendations to the ICBM
4. Ensure that annual reviews of the risks to ARINC corporate information and related information systems are conducted by the ISSM
5. Review any remedial actions taken to reduce ARINC exposure upon identification of new security threats
6. Review waiver recommendations from Business Units concerning Information Systems Security Policies and act as the final authority on decisions for resolution of such requests. The ECCB shall direct and review risk assessments.
7. Ensure that annual reports generated by the ISSM reflecting Information Systems Security status and progress are submitted to the ICBM
8. Ensure Information Systems Security waiver requests (including risk assessments and recommendations for risk mitigation) are adjudicated
9. Coordinate actions taken in response to security incidents with the ICBM
10. Perform other necessary high-level Information Systems Security management activities as directed by the ICBM

1.3.6 Users

Each ARINC User shall:

1. Comply with the Information Systems Security Policies.
2. Exercise good judgment and apply sound security principles.
3. Safeguard all personal access capabilities and login privileges.
4. Promptly report suspected Information Systems Security breaches or issues to the appropriate System Administrator. If the administrator is not known, not responsive or unavailable, Users must promptly report such breaches or issues to their division security point of contact.

Every ARINC user is prohibited from:

1. Disclosing to any non-ARINC person or entity either the nature of in-place or planned Information Systems Security controls or the details surrounding such controls.
2. Testing, or attempting to compromise internal security controls unless specifically approved in advance and in writing by the ECCB. System Administrators of multi-user systems will be pre-authorized to test their systems using approved procedures.
3. Using or possessing software or hardware tools designed to test or compromise security control mechanisms unless specifically authorized in writing by the ECCB.
4. Introducing non-company owned computers, computer peripherals, or computer software into ARINC facilities, or entrusting company data to such devices, without proper authorization from the Business Unit Representative.
5. Using an E-mail or Voice-mail account assigned to another individual. Where there is legitimate need to have a person access another person's mail (administrative assistant, vacation coverage, etc.), then such individual shall be a responsible ARINC employee and message forwarding, delegation features, or other system facilities that preserve individual accountability shall be used.

1.4 Provision of Authority

ARINC Engineering Services, LLC issues this plan. Authority is granted to the Program Manager to update this plan if necessitated by concerns of IT security resulting from reviews or changes in NASA IT Security Policy/Regulations throughout the life of this contract.

This plan is based on the established procedures outlined in NASA Procedural Requirements (NPR) 2810.1, *Security of Information Technology* and the ARINC IT Security Policies, which are available online to all employees and onsite contractors. All contract tasks that are conducted by ARINC team personnel at NASA facilities shall comply with applicable NASA center requirements.

1.4.1 ARINC Documents

Bulletin #6200, Information Systems Security
Bulletin #6210, Privilege Control
Bulletin #6220, Auditing & Logging
Bulletin #6230, Network Security
Bulletin #6250, System Security
Bulletin #6260, Intrusion Response & Recovery

1.4.2 Federal Government Documents

Public Law (PL) 93-579 (12/31/74), "Privacy Act of 1974."
PL 100-235, "Computer Security Act of 1987."
22 CFR Parts 120-130, "International Traffic in Arms Regulations" (ITAR)

1.4.3 OMB Documents

OMB Circular A-130, "Management of Federal Information Resources"

1.4.4 NASA Documents

NASA Policy Directive (NPD) 2810.1, "Security of Information Technology"
NASA Procedural Requirements (NPR) 2810.1A, "Security of Information Technology"

2. Information Technology System Types

2.4.1 The NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories, will assist in understanding the relationship between categorization and system types. The OMB Circular A-130, Appendix III requires that Federal information systems be categorized into two types of systems, major applications (MA) and general support systems (GSS). Homeland Security Presidential Directive (HSPD) 7, Critical Infrastructure Identification, Prioritization, and Protection, establishes a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks. In NPR 1600.1, NASA Security Program Procedural Requirements, 8.4, NASA Critical Infrastructure and Key Resources, NASA has elected to designate its critical infrastructure and key resources as Mission Essential Infrastructure (MEI) to better facilitate designation of vital "mission-oriented" critical infrastructure and key resources.

2.4.1.1 Major Application (MA). An MA system is an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of, the information in the application. A breach in an MA has the potential to compromise many individual application programs

and hardware, software, and telecommunications components. MA systems can be either a major software application or a combination of hardware/software where the only purpose of the system is to support a specific mission-related function.

2.4.1.2 General Support System (GSS). A GSS system is an interconnected information resource under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, facilities, and people. A system can be, for example, a local area network (LAN) including smart terminals that supports a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization (IPSO).

2.4.1.3 NASA Critical Infrastructure and Key Resources--MEI Protection Program. Homeland Security Presidential Directive (HSPD) 7, Critical Infrastructure Identification, Prioritization, and Protection, directs agencies to establish a program to identify critical infrastructure and key resources, evaluate these assets for vulnerabilities, and fund and

3. TECHNICAL SECURITY REQUIREMENTS

3.1 Operating System Integrity

This section describes the requirements for ensuring operating system integrity on multi-user computers under NASA's purview.

3.1.1 Critical System Files Protection

Critical system files are those that are integral to the operating system, system security mechanisms, or key system services. Corrupting these files would damage the integrity of the system.

3.1.1.1 BRT Information Category

Critical file protection processes shall:

a. Control file access
b. Identify and protect critical system files
c. Restrict access to critical system files to a minimum number of authorized system support personnel
d. Restrict access to password files to user identification (ID) management personnel
e. Review critical system file protection at least semiannually
f. Implement configuration control for critical system files
g. Maintain a list of authorized users of critical system files and verify the list at least semiannually

3.1.1.2 SER and ADM Information Categories

Critical file protection processes shall:

a. Control file access
b. Identify and protect critical system files
c. Restrict access to critical system files to authorized users
d. Restrict access to password files
e. Review critical system file protection at least annually

3.1.1.3 PUB Information Category

Critical file protection processes shall ensure implementation of requirements as directed by the applicable NASA Center's security policies, procedures, and guidelines.

3.1.2 Privileged Users and Programs

A privileged user is one who can alter or circumvent the operating system or the system's security protections. This applies to users who may have only limited privileges but who can still bypass security protections. The following requirements for privileged users and programs shall be implemented for IT systems under NASA's purview.

3.1.2.1 BRT, SER, and ADM Information Categories

The processes controlling privileged users and programs shall:

a. Assign operating system privileges to a minimum number of systems personnel
b. Control access to privileged programs
c. Maintain a list of privileged users and verify the list at least semiannually
d. Ensure that system administration/support personnel do not function as system auditors

3.1.2.2 PUB Information Category

The processes controlling privileged users and programs shall:

a. Assign operating system privileges to a minimum number of systems personnel

b. Ensure implementation of additional requirements as directed by the NASA Center's security policies, procedures, and guidelines

3.1.3 Journaling and Monitoring

Multi-user computers under NASA's purview have the ability to record or journal important system events. These journals can be used as an audit trail to investigate system or security problems.

3.1.3.1 BRT Information Category

Journaling and Monitoring processes shall:

a. Ensure system journals record security-related events unless specifically waived by the functional manager of the application software
b. Review journals weekly (or more frequently when problems are suspected)
c. Record successful and failed logons/logoffs
d. Record all successful and failed file opens and closes at the discretion of the line manager
e. Record critical system file modification events or attempts
f. Ensure journals identify programs being executed, users, source devices, files, and the time, date, and success or failure of all access attempts

3.1.3.2 SER and ADM Information Categories

Journaling and Monitoring processes shall:

a. Implement system journals to record security-relevant events as directed by management
b. Review journals monthly or more frequently when problems are suspected
c. Record successful and failed logons/logoffs
d. Record critical system file modification events
e. Ensure journals identify programs being executed, users, source devices, files, and the time, date, and success or failure of access attempts

3.1.3.3 PUB Information Category

Journaling and Monitoring processes shall ensure implementation of requirements as directed by the NASA Center's security policies, procedures, and guidelines

3.1.4 System Retention/Backup

To ensure continuity of operation of IT systems under NASA's purview, copies of important software and data will be made and retained.

3.1.4.1 BRT Information Category

System retention/backup procedures shall require system administration to:

a. Retain journals for at least 6 months
b. Back up the operating system and key system services monthly and when modified
c. Retain monthly operating system backups for at least 6 months
d. Store the most recent or most recent minus one backup external to the facility

3.1.4.2 SER, ADM, PUB Information Categories

System retention/backup procedures shall require system administration to retain journals and backup system as directed by the line manager

3.1.5 System Shutdown/Restart

IT systems under NASA's purview shall provide security safeguards to cover unscheduled system shutdowns (e.g., aborts) and subsequent restarts as well as for scheduled system shutdown and operational startup.

3.1.5.1 BRT Information Category

System Shutdown/Startup procedures shall ensure that:

a. System shutdown/restart procedures are documented
b. Only authorized personnel will shutdown/restart the system
c. All aborts and restarts are logged and document

3.1.5.2 SER and ADM Information Categories

System Shutdown/Startup procedures shall ensure that:

a. System shutdown/restart procedures are documented
b. Only authorized personnel will restart the system

3.1.5.3 PUB Information Category

System Shutdown/Startup procedures shall ensure implementation of requirements as directed by the NASA Center's security policies, procedures, and guidelines.

3.1.6 Operating System Local Modifications

Local modifications to the operating system can have security implications. The following local system modification requirements shall apply to all IT systems under NASA's purview.

3.1.6.1 BRT Information Category

Operating system modification procedures shall require:

a. Review and approval of all operating system security modifications
b. Test and/or evaluation of all operating system modifications for impact on security before permanent installation
c. Documentation of all operating system security modifications

3.1.6.2 SER, ADM, and PUB Information Categories

Operating system modification procedures shall require documentation of all operating system security modifications as directed by the line manager.

3.1.7 Configuration Management

Because the operating system governs the security of the system, changes to the operating system, including new releases and updates, of NASA IT resources or systems shall be controlled and monitored.

3.1.7.1 BRT Information Category

Configuration Management processes for operating system modifications shall require:

a. Documentation of change control for critical system files
b. Test, evaluation, and documentation of all operating system changes

3.1.7.2 SER, ADM, and PUB Information Categories

Configuration Management processes for operating system modifications shall require test and documentation all operating system changes as directed by the line manager.

3.2 User ID Management

A user ID is a character string that uniquely identifies a user. The NASA requirements to be implemented for user ID management are listed in the following paragraphs. User ID management applies to all NASA processing environments.

3.2.1. User ID Approval Process/Privileges

Control processes shall be implemented to ensure that all requests for user ID's are reviewed and approved by NASA line management. A list of personnel who are authorized to approve the user ID's will be furnished to the appropriate user-ID administrator.

3.2.1.1 BRT Information Category

User ID approval processes shall:

a. Ensure that each employee submits a formal request to the appropriate administrator for a user ID (The request will indicate the category of the user ID being requested, such as group, personal, privileged, project, application system service, or generic.)
b. Ensure verification of personnel screening and IT security briefing
c. Approve the formal request by the employee's manager (and NASA sponsor for access to NASA systems or network)
d. Require all individuals assigned a user ID to sign a statement of responsibility indicating their understanding of the requirements for using and safeguarding the information to which the assigned user ID grants access
e. Retain the statement of responsibility by user ID management for every active account

3.2.1.2 SER and ADM Information Categories

User ID Approval processes shall require all individuals requesting a user ID to complete the appropriate request form and sign a statement of responsibility indicating their understanding of the requirements for using and safeguarding the information to which the assigned user ID is granted access

3.2.1.3 PUB Information Category

User ID Approval processes shall require controls as directed by the line manager.

3.2.2. Group User ID's

Group user ID's for NASA IT systems are discouraged because individual accountability is lost. However, if the system is configured such that group user ID's must be used, the processes shall be implemented that accomplish the following:

3.2.2.1 BRT Information Category

a. Do not provide group user ID's without risk justification and concurrence from all functional managers of the affected data and applications
b. Restrict group user ID's to the minimum number necessary to conduct system operations

3.2.2.2 SER and ADM Information Categories

Restrict group user ID's to the minimum number necessary to conduct system operations

3.2.2.3 PUB Information Category

Permit group user ID's only as directed by the NASA Center's security policies, procedures, and guidelines

3.2.3. User ID Revalidation

An inventory of all assigned NASA IT system user ID's shall be maintained for all information categories.

3.2.3.1 BRT, SER, and ADM Information Categories

a. All user ID's shall be revalidated at least annually
b. A statement of responsibility shall be on file for each person who has a user ID

3.2.3.2 PUB Information Category

User IDs shall be revalidated as directed by the NASA Center's security policies, procedures, and guidelines

3.2.4. Disposition of Unused User ID's

Proper disposition shall be required for all unused NASA IT system user ID's. User ID disposition uses password lifetime (i.e., the number of days before users receive reminders to change their passwords) as the metric for user-ID-deletion decisions. The table below identifies the maximum lifetimes (in calendar days) before a user ID is removed from the system.

Info Category	Number of days before user receives reminders to change password	Number of days that user will be reminded to change password	Number of days until user ID is suspended if user does not change password	Number of days until user ID is removed from the system
BRT	60 days	+ 30 days	90 total days	180 total days
SER, ADM	90 days	+ 30 days	120 total days	240 total days
PUB	As determined by the line manager			

3.2.5. User ID Reuse

3.2.5.1 BRT Information Category

User ID's may be reassigned after removal from the system when all access rights and privileges associated with the user ID have been removed.

3.2.5.2 SER, ADM, and PUB Information Categories

Reassignment of User ID shall be in accordance with directives provided by the line manager.

3.2.6. Notification upon Termination

3.2.6.1 Termination for Cause or Reduction in Force.

A user's supervisor will notify the manager of all NASA IT systems on which the user holds a user ID when that individual is terminated for cause or reduction in force:

a. As soon as practical but no later than the end of the day of the termination for BRT information category
b. Within 2 working days of the termination for SER, ADM, and PUB information categories

3.2.6.2 Resignation/Change of Job/Retirement

A user's supervisor will notify the manager of all NASA IT systems on which the user holds a user ID when that individual retires, or is transferred:

a. Within 5 working days for the BRT information category
b. Within 15 working days for the SER, ADM, and PUB information categories

In addition, the user's supervisor is responsible for the disposition of user IDs for users who no longer needs to access the system to perform assigned duties. Time limits for disposition of such user ID's is at line management's discretion, based on each individual case.

3.3. Passwords

Users are responsible for any and all activity generated through the use of their user ID's and passwords. NASA IT resources, which use passwords for user authentication, shall meet the password standards defined in this section. Users shall not store passwords in program function keys or automated logon sequences.

3.3.1. Individual Accountability

Each individual shall be accountable for providing protection against loss or disclosure of passwords in his or her possession. Individuals shall accept responsibility for all activity that occurs as a result of deliberately revealing his or her user ID and password.

3.3.2. Password Length and Composition

Passwords shall consist of a minimum of eight characters. The eight characters will contain at least one character each from at least three of the following sets of characters: uppercase letters, lowercase letters, numbers, and special characters.

3.3.3. Password Triviality

Only nontrivial passwords shall be used. A password is considered nontrivial if it meets the following criteria:

a. The password is not equal to the user ID.
b. The password is not a dictionary word.
c. The password is not either wholly or predominantly composed of the following:
    (1) The user's ID, owner's name, birth date, Social Security Number, family member or pet names, names spelled backwards, or other personal information about the user
    (2) Any contractor name
    (3) The division or branch name
    (4) Repetitive or keyboard patterns (e.g., "abc#abc#", "1234", "qwer", "mnbvc", or "aaa#aaaa")
    (5) The name of any automobile or sports team

d. The password is not a word found in a dictionary of any language or a dictionary word with numbers appended or prepended to it.
e. The password is not the name of a vendor product or a nickname for a product.

3.3.4. Password Maximum Lifetime

Password lifetime requirements shall be:

a. 90 days maximum for BRT information category
b. 1 year maximum for SER and ADM information categories
c. 1 year maximum for PUB information category

3.3.5. Password Sharing

Password sharing shall be discouraged for all information categories. Password sharing requirements shall be as follows:

BRT Information Category

a. Personal passwords used to authenticate identity will be owned (i.e., known) only by the individual having that identity.
b. The user ID owner may employ system features (e.g., logonby or the equivalent) to grant temporary access to another individual.

SER, ADM, and PUB information Categories

a. Personal passwords used to authenticate identity will be owned (i.e., known) by only the individual having that identity.
b. The user ID owner may employ system features (e.g., logonby or the equivalent) to grant ongoing access to another individual or may create a temporary password.

3.3.6. Password Reuse

Password reuse shall be discouraged for all information categories. Password reuse requirements shall be as follows:

BRT Information Category

a. Owner must have used a minimum of 10 passwords before reuse
b. 180 days must elapse before reuse

SER, ADM, and PUB information Categories

Password reuse requirements shall be as directed by the NASA Center's security policies, procedures, and guidelines.

3.3.7. Password Storage

The following password storage requirements shall be implemented:

MSN, BRT, SER, and ADM Information Categories

a. Stored passwords will be protected in such a way that only the password system is authorized access to a password.
b. Passwords that are encrypted before they are stored will be protected from substitution (i.e., protection will be provided so that one encrypted password cannot be replaced with another unless the replacement is authorized).

PUB Information Category

Password storage requirements shall be in accordance with the NASA Center's security policies, procedures, and guidelines.

3.3.8. Password Distribution

BRT Information Category

The password distribution system shall:

a. Distribute personal passwords in a way that affords reasonable protection from unauthorized disclosure
b. Distribute passwords in such a way that temporary storage of the password is erased, and long-term retention of the password is available only to the owner and the protected password system
c. Ensure that passwords are not visible at the user terminal when being typed
d. Distribute passwords so that an audit record, containing the user ID, date, and time of a password change, is maintained and available only to authorized personnel

SER and ADM Information Categories

The password distribution system shall:

a. Distribute personal passwords in a way that affords reasonable protection from unauthorized disclosure
b. Distribute passwords in such a way that temporary storage of the password is erased, and long-term retention of the password is available only to the owner and the protected password system
c. Ensure that passwords are not visible at the user terminal when being typed
d. Distribute passwords so that an audit record, containing the user ID, date, and time of a password change is maintained and is available only to authorized personnel

PUB Information Category

Password distribution shall be as directed by the line manager.

3.3.9. Password Reset

Passwords are reset when a user forgets his or her password, when evidence exists that a password has been compromised, or when management believes a password reset to be in the best interests of the security of the system. For all information categories, the password reset process shall require:

a. Confirmation of name, location, phone number, and system user ID of the user needing reset
b. Positive identification of the user ID owner
c. Assignment, at the user's request, a new nontrivial password
d. Password reset by the user during first sign-on

3.3.10. Initial Passwords

The process for generating and assigning the initial password for each user ID shall include the following for all information categories:

a. Removal of all vendor-supplied passwords
b. Assignment of nontrivial initial user password
c. Initial user password change during the first logon by the user

3.4. Logical Access Control for Multi-User Systems

Logical access control is the process of limiting access to the resources of the system to authorized users, programs, processes, or other systems. This section applies to multi-user systems under NASA's purview. Logical access controls also apply to networks. Network security requirements are presented in section 4.

3.4.1. User Authentication

User authentication is the process by which the system verifies the user's claim of identity. The user shall authenticate his or her identity by presenting to the system some piece of information that is his or hers: either something known (password), something possessed (a key or token), or something he or she is (such as a biometrics measurement).

3.4.1.1 Local Logons (i.e., log on directly to a system)

a. BRT, SER, and ADM Information Categories shall require user identification and local authentication (at least passwords) for all user ID's.
b. PUB Information Category shall require user identification as directed by the line manager

3.4.1.2 Remote logons

a. BRT, SER, and ADM information categories shall permit remote authentication, at the discretion of the remote System Administrator, when:
   - The authenticating system meets all appropriate security requirements of the remote system
   - The authenticating mechanism creates audit trails
   - The risk of subverting the connection between the remote and local systems is acceptable to the remote System Administrator
b. PUB Information Category shall require user identification as directed by the line manager

3.4.2. Failed Logon Attempts

Failed logon attempts are unsuccessful attempts to provide the correct logon user ID and authentication combination.

3.4.2.1 BRT Information Category

The system administration processes shall:

a. Suspend the user ID after five or fewer unsuccessful logon attempts or provides some form of system evasive action
b. Notify the System Administrator of user ID suspensions
c. Review the log of unsuccessful logon attempts weekly
d. Notify the user ID owner of failed logon attempts

3.4.2.2 SER and ADM Information Category

The system administration processes shall:

a. Ensure system intervention on the user ID after five or fewer successive unsuccessful logon attempts (The line manager and IT security personnel will determine the system intervention action taken.)
b. Review the log of unsuccessful logon attempts weekly
c. Notify the user ID owner of failed logon attempts

3.4.2.3PUB Information Category

The system administration processes shall provide failed logon attempt requirements as directed by the NASA Center's security policies, procedures, and guidelines.

3.4.3. Controlled Access Protection

Controlled access protection is the ability of the NASA IT system to control the circumstances under which users have access to resources.

3.4.3.1 BRT, SER, ADM Information Categories

Multi-user systems shall provide the following controlled access protection:

a. Individual electronic accountability through identification and authentication of each system user
b. Audit trails or a journal of security-relevant events
c. Ability to control a user's access to information

3.4.3.2 PUB Information Category

Multi-user systems shall provide controls as directed by the NASA Center's security policies, procedures, and guidelines

3.4.4. Default File Protection

Default file protection is access control the system places on a file when the data owner does not take explicit action.

3.4.4.1 BRT Information Category

Default file protection shall:

a. Set system default file protection parameters to grant write access to the file owner and to necessary operating system components
b. Set system default file protection parameters to prevent read and execute access by anyone except the file owner and necessary operating system components

3.4.4.2 SER and ADM Information Category

Default file protection shall set system default file protection parameters to grant write and execute access to the file owner and to necessary operating system components

3.4.4.3 PUB Information Category

Default file protection shall implement requirements as directed by the NASA Center's security policies, procedures, and guidelines.

3.5. Information Management and Protection for Multi-User Computers

For multi-user computers under NASA's purview, the applicable information category shall be established according to the following:

- Applications shall derive information category designation from the data processed or contained
- The computer system shall derive derives information category level designation from the applications handled or stored

Information owners shall determine protection and sharing requirements. Owners shall either apply the protections themselves or designate other appropriate personnel, such as data custodians or System Administrators, to implement protections.

Software tools used to develop and support specific applications shall be owned by the application owner. Tools that are shared by all system users (such as a language compiler) are owned by the group with the primary responsibility for the host system.

3.5.1. Data Owner Requirements/Responsibilities

3.5.1.1 BRT Information Category

The data owner shall:

a. Specify the information category of the application/information (subject to review by the NASA Center IT Security Manager)
b. Specify the security protections to be implemented
c. Identify authorized users and custodians
d. Identify and protect private data from unauthorized disclosure
e. Ensure that hard copy output (including electronic media) is controlled as necessary
f. Ensure that implementation of file access controls as appropriate

3.5.1.2 SER and ADM Information Categories

The data owner shall:

a. Specify the information category of the application/information (subject to review by the NASA Center IT Security Manager)
b. Specify the security protections to be implemented
c. Identify authorized users and custodians, as appropriate
d. Protect private data from unauthorized disclosure

3.5.1.3 PUB Information Category

The data owner shall ensure that implementation of requirements as directed by the NASA Center's security policies, procedures, and guidelines

3.5.2. Application Data Backup /Recovery

Application data backup/recovery defines the owner's requirements to restore the application/information after a system (hardware/software) malfunction or compromise of integrity.

3.5.2.1 BRT Information Category

The application owner shall ensure that:

a. At least three generations of backups are retained
b. The most recent (or most recent minus one) backup is stored in an external facility
c. Frequency of application data backups is defined
d. Data recovery procedures are defined and tested

3.5.3.2 SER, ADM, and PUB Information Categories

The application owner shall ensure that requirements are implemented as directed by the NASA Center's security policies, procedures, and guidelines

3.6. Commercial Off-the-Shelf (COTS) Software

COTS software is software that has been developed, tested, placed on the market, and advertised as a saleable product. Before installation on NASA IT systems, COTS software will be tested on the system according to the requirements in paragraph 3.6.1. Maintenance of COTS software will be done according to the requirements in paragraph 3.6.2.

3.6.1. Software Acceptance Testing

Software acceptance testing for IT security features provides a measure of assurance that the software product correctly provides the advertised capabilities.

3.6.1.1 BRT Information Category

Acceptance testing procedures for IT security features shall ensure that:

a. Testing or inspection of available source code is performed to ensure that the program and installation scripts are free from malicious or unauthorized code.
b. Function, reliability, and penetration tests are included in a test plan and performed.
c. Testing and verification of security controls and application features are witnessed by appropriate personnel and documented.

3.6.1.2 SER and ADM Information Categories

Acceptance testing procedures for IT security features shall ensure that tests are performed that show the program is free from malicious or unauthorized code (e.g., scanning for known viruses, backdoors, logic bombs , and Trojan code)

3.6.1.3 PUB Information Category

Acceptance testing procedures for IT security features shall ensure that tests, as directed by the NASA center's security policies, procedures, and guidelines, are conducted.

3.6.2. Maintenance of COTS Software

Software maintenance (i.e., modifications and updates) increases the risk that errors, accidents, and intentional acts can occur.

3.6.2.1 BRT Information Category

COTS Software Maintenance processes shall require:

a. Review, evaluation, installation, and test of all vendor-recommended application updates in accordance with paragraph 3.6.1
b. Control by a configuration management process

3.6.2.2 SER, ADM, and PUB Information Categories

COTS Software Maintenance processes shall require implementation requirements as directed by the NASA Center's security policies, procedures, and guidelines

3.7. Public Domain Software

Public domain software includes software acquired from the Government or non-government sources, often at no charge, when the source takes no responsibility for the integrity or maintenance of the software. The following security requirements shall apply to implementation of public domain software for IT systems under NASA's purview.

3.7.1. User Workstations

3.7.1.1 BRT Information Category

a. All public domain workstation software shall be approved by an officially appointed staff member who will ensure that the software is free of malicious code before installation.
b. All solicited or unsolicited sample programs shall be approved by an officially appointed staff member who will ensure that the software is free of malicious code before installation.

3.7.1.2 SER, ADM, and PUB Information Categories

All workstation software not acquired through the normal Center procurement processes shall be approved before installation in accordance with requirements established by the staff element in question.

3.7.2. Mainframes

3.7.2.1 BRT Information Category

a. All public domain mainframe software shall be approved by an officially appointed staff member who will ensure that the software is free of malicious code before installation.
b. All solicited or unsolicited sample programs shall be approved by an officially appointed staff member who will ensure that the software is free of malicious code before installation.

3.7.2.2 SER, ADM, and PUB Information Categories

All mainframe public domain software not acquired through normal Center procurement processes shall be approved before installation in accordance with requirements established by the staff element in question.

3.8. Customer/Contractor-Supplied Software

Customer/contractor-supplied software is software that is developed or customized by either in-house or contractor-supplied services, including universities. The following security requirements shall apply to implementation of customer-/contractor-supplied software for IT systems under NASA's purview.

3.8.1. Formalized Project Life-Cycle Development

Each line manager engaged in formal life-cycle project development will ensure that basic security requirements are integrated throughout the software's life cycle.

3.8.1.1 BRT, SER, and ADM Information Categories

a. Establish security requirements for applications
b. Review decisions on implementation of security controls during definition, design, programming, and testing
c. Review and enforce operational security controls

3.8.1.2 PUB Information Category

Review and enforce operational security controls

3.9. Encryption of Unclassified Data

Encryption shall to be used on sensitive/critical data for NASA IT systems when the risk analysis process for that system so dictates. When encryption is required, the algorithm specified in FIPS 46-1, currently the Data Encryption Standard (DES), will be used for production systems.

3.9.1. Requirement

The responsible task manager shall implement a process for all applicable information categories that:

a. Ensures that a key management process is established and maintained
b. Ensures that a data recovery process is maintained to ensure that NASA information is accessible

Encryption of data at this level is not normally applicable to PUB Information Category

3.9.2. Key Management

Key management refers to the generation, distribution, storage, and destruction of keys used to encrypt and decrypt data. The responsible task manager shall implement a process for all applicable information categories that:

a. Affords electronically stored cryptographic keys the same level of security
b. Designates and records a key owner for each cryptographic key
c. Ensures that the key owner distributes the cryptographic key to authorized personnel only
d. Delivers the cryptographic key to its recipients in a manner that is at least as secure as logon password distribution

Encryption of data at this level is not normally applicable to PUB Information Category.

3.9.3. Password Encryption

3.9.3.1 BRT, SER, and ADM Information Categories

The responsible task manager shall implement a process that:

a. Encrypts passwords if it is possible for either privileged or nonprivileged users to browse memory or storage media where passwords are kept
b. Encrypts password files on backup storage media if it is possible for either privileged or nonprivileged users to browse the media

3.9.3.2 PUB Information Category

The responsible task manager shall implement a process that:

a. Encrypts passwords if directed by the Center's security policies, procedures, and guidelines
b. Encrypts passwords if the system on which they are used is connected to a system of higher sensitivity

3.9.4. Private Data

Private data are data that has disclosure restrictions such as Privacy Act , source selection, contractor proprietary, or medical data. The responsible task manager shall implement a process for all applicable information categories that:

a. Encrypts private data if the system has no other mechanism for providing controlled browse access protection to the data

b. Encrypts private files on backup tapes if the tape library system has no other mechanism for providing controlled browse access protection to the data

Note: "Browse access protection" may be provided by appropriate physical security measures for systems without external interfaces.

Encryption of data at this level is not normally applicable to PUB Information Category.

3.10. Centralized Operations for Multi-User Systems, Servers, and Mainframes

Centralized operations for NASA IT resources or systems refer to the operational tasks and ancillary functions that support multi-user systems, servers, and mainframes (also known as host systems). Operational tasks include the setup, operations (e.g., start, stop, configure, bypass/recover), and monitoring of console control units and peripherals. Operational tasks may be accomplished from a centralized location or a remote console. Ancillary tasks include job and event scheduling and processing, job quality control, magnetic tape cleaning and certification, magnetic disk module inspection and cleaning, tape library operation, and the coordination of media retention and accountability tasks.

3.10.1. Documentation

BRT Information Category

The responsible task manager will implement a process that:

a. Retains complete operating system and appropriate application documentation
b. Develops, uses, and maintains operating procedures and checklists
c. Maintains a complete inventory of system software and application software
d. Maintains and reviews a list of system security software problems as directed by management
e. Reviews applications annually for changes in information categories
f. Develops and maintains risk analysis , risk reduction, and contingency plans
g. Maintains a list of personnel responsible for system and application software

SER and ADM Information Categories

The responsible task manager will implement a process that:

a. Retains complete operating system documentation
b. Develops and maintains operating procedures and checklists
c. Maintains a complete list of systems' applications
d. Maintains and reviews a list of system security software problems as directed by management
e. Reviews applications annually for changes in information categories
f. Develops and maintains risk analysis , risk reduction, and contingency plans
g. Maintains a list of personnel responsible for system and application software

PUB Information Category

The responsible task manager will implement a process that:

a. Reviews applications annually for changes in information categories
b. Maintains a list of personnel responsible for system and application software
c. Maintains documentation as required by the NASA Center's security policies, procedures, and guidelines

3.10.2. Privileged Operations

3.10.2.1 BRT, SER, and ADM Information Categories

The responsible task manager shall implement a process that:

a. Controls access to operator consoles
b. Ensures that operators do not transfer privileged activity outside the operations area without proper authorization
c. Ensures that only the operations group is authorized to disable console logging and that the event is logged when performed
d. Documents and reports IT security incidents to the Organization Computer Security Official, management, and NASA Center IT Security Manager
e. Maintains and archives (both manual and automatic) console logs
f. Reviews operator console logs regularly

3.10.2.2 PUB Information Category

a. The responsible task manager shall implement a process that:
b. Controls access to operator consoles
c. Ensures that operators do not transfer privileged activity outside the operations area without proper authorization
d. Ensures that only the operations group is authorized to disable console logging and that the event is logged when performed
e. Documents and reports IT security incidents to the Organization Computer Security Official, management, and NASA Center IT Security Manager

3.10.3. Console Logon

3.10.3.1 BRT, SER, and ADM Information Categories

The responsible task manager shall implement a process that:

a. Ensures that operators do not transfer privileged activity outside the operations area without proper authorization
b. Ensures that only the operations group is authorized to disable console logging and that the event is logged when performed
c. Documents and reports IT security incidents to the Organization Computer Security Official, management, and NASA Center IT Security Manager
d. Maintains and archives (both manual and automatic) console logs
e. Reviews operator console logs regularly

3.10.3.2 PUB Information Category

The responsible task manager shall implement a process that:

a. Ensures that only the operations group is authorized to disable console logging and that the event is logged when performed
b. Documents and reports IT security incidents to the Organization Computer Security Official, management, and NASA Center IT Security Manager
c. Reviews operator console logs regularly

3.10.4. Media Storage

Media may be stored in a variety of environments, including libraries, offices, laboratories, and computer rooms. Whenever it is stored, the media shall be protected from destruction, damage, theft, unauthorized modification, and unauthorized access.

3.10.4.1 BRT Information Category

Operations management shall implement a process that:

a. Ensures that the media library is in an environmentally controlled area
b. Ensures that only authorized personnel have access to the media
c. Provides an inventory accounting system for all media entering or leaving a media storage facility when appropriate
d. Maintains and verifies a media inventory at least semiannually
e. Identifies all media with an external label and, when applicable, an internal label
f. Provides a visual means of identification (i.e., labels) for all media containing private data
g. Ensures that media containing restricted access data are degaussed (erased)/overwritten before being disposed or returned to use
h. Protects media from theft, vandalism, and natural disasters

3.10.4.2 SER and ADM Information Categories

Operations management shall implement a process that:

a. Ensures that the media are in an environmentally controlled area
b. Ensures that only authorized personnel access the media
c. Ensures that media containing restricted access data are degaussed (erased)/overwritten before being returned to use or disposed
d. Protects media from theft, vandalism, and natural disasters

3.10.4.3 PUB Information Category

Operations management shall implement a process that: protects media from theft, vandalism, and natural disasters.

3.10.5. Job Input

Whenever operations personnel are required to set up and process job input to support a customer or user, operations management will implement a process that:

a. Ensures that input comes from an authorized source for BRT, SER, and ADM information categories
b. Ensures the implementation of requirements as directed by the NASA Center's security policies, procedures, and guidelines for PUB information category

3.10.6. Job Output

3.10.6,1 BRT, SER, and ADM Information Categories

To ensure the continued protection of the information after it leaves the processing area, operations management shall implement a process that:

a. Attaches the appropriate cover sheet to all output containing private data
b. Distributes restricted access output to only authorized personnel

c. Destroys any restricted access data that has not been distributed after a time period specified by task manager

3.10.6.2 PUB Information category

To ensure the continued protection of the information after it leaves the processing area, operations management shall implement a process that ensures the implementation of requirements as directed by the NASA Center's security policies, procedures, and guidelines.

3.11. Workstation Security Requirements

Workstations include systems used to support desktop processing (personal computers), LAN's, and servers typically used in an office or laboratory environment.

3.11.1. Single-User Workstations

A single-user NASA workstation is one that may be used by only one person at a time, though many people may have access.

3.11.1.1 BRT, SER, ADM Information Categories

The responsible task manager shall implement a process that:

a. Implement a risk management program commensurate with the information category being processed
b. Establish backup and recovery requirements
c. Ensure that virus detection software is installed on all applicable workstations

3.11.1.2 PUB Information Category

The responsible task manager shall implement a process that:

a. Ensures that system configuration is documented
b. Establishes backup requirements
c. Ensures that virus detection software is installed on all applicable workstations

3.11.2. Multi-user Workstations

A multi-user NASA workstation can be accessed simultaneously by other workstations.

3.11.2.1 BRT Information Category

Where multi-user workstations are installed, the responsible task manager will implement a process that:

a. Documents system configuration
b. Ensures that virus detection software is installed in the workstation where applicable
c. Ensures that backup requirements are established
d. Implements a risk management program appropriate for the category being processed
e. Assigns a System Administrator
f. Identifies each user by a unique user ID and password
g. Provides secure backup storage external to the processing area
h. Ensures that critical data backups are placed in secure storage

3.11.2.2 SER and ADM Information Categories

Where multi-user workstations are installed, the responsible task manager will implement a process that:

a. Documents system configuration
b. Ensures that virus detection software is installed in the workstation where applicable
c. Ensures that backup requirements are established
d. Develops a contingency plan

3.11.2.3 PUB Information Category

Where multi-user workstations are installed, the responsible task manager will implement a process that:

a. Documents system configuration
b. Ensures that virus detection software is installed in the workstation where applicable
c. Establishes backup requirements

3.12. Authorization to Process (or Certification/Recertification)

Each NASA IT system that processes information by or on behalf of the Federal Government shall have written authorization and periodic re-authorization to process by the appropriate line management official.

a. The authorization and periodic re-authorization shall take the form of a letter to the NASA Center IT Security Manager summarizing the results of the risk analysis; any residual risk; planned, budgeted, and scheduled corrective actions; and a certification statement of risk acceptance to process. For small systems, a cover letter or an approval sheet with the signatures of the responsible line manager and any affected "data owners" attached to the IT Security Plan can be used.
b. The authorization and periodic re-authorization are required in writing upon attaining initial operational capability and at least every 3 years (or upon significant change) thereafter before the system is permitted to process or continue to process information.
c. Copies of the authorization and re-authorization will be filed with the NASA Center IT Security Manager.

4. NETWORK SECURITY REQUIREMENTS

This section includes network security guidelines and baseline requirements for NASA networks. These requirements supplement the requirements of any individual systems connected to the network (sometimes referred to as network nodes or hosts).

4.1 Network Security Elements

The security of a network or any attached node consists of three elements: integrity (e.g., ensuring that transmitted data is received intact), availability (e.g., network services are performed within an acceptable timeframe), and confidentiality (e.g., preserving the privacy of information).

4.1.1 Network Data Integrity

Information transmitted over the network shall be protected during transmission from unauthorized modification, whether by accident, error, or willful alteration. NASA networks provide integrity through the use of established protocols and network devices with proven error detection capabilities.

4.1.2. Network Availability

Network availability depends on protection against loss of or damage to network components and network abuse. NASA's networks are protected from damage to, or loss of, network

components by physically protecting components and providing redundant connections. Protective measures against network abuse include user authentication and network monitoring. Availability and integrity are security concerns as well as operational concerns. The loss of availability and integrity due to equipment failure or improper maintenance is beyond the scope of this plan.

4.1.3. Network Confidentiality

Types of information that require privacy protection are passwords, which could be captured and used to gain unauthorized access to NASA computers; personnel records, which are protected by the Privacy Act; financial data, such as payroll information; sensitive electronic mail, such as performance evaluations; proprietary, contract, or other data dealing with procurements, such as source selection information; and other data with restrictions on its distribution, such as export controlled information. Protective measures shall be employed when private data must be transmitted over networks. The scope and cost-effectiveness of protection shall be the responsibility of the task manager and shall be based on the results of the risk assessment.

4.2 Establishing a Network Security Architecture

All unclassified networks under NASA's purview shall use a network architecture that addresses network security concerns. The responsible task manager or network administrator shall:

a. Implement safeguards to protect information resources, including the network's equipment, against misuse or attack to a level commensurate with their importance
b. Identify the goals and priorities for network operations such as:
   - Protecting Government resources
   - Maintaining operational support requirements and network connectivity at an acceptable level of risk
   - Supporting legal or administrative enforcement efforts
c. Assign a LAN Manager who is responsible for network operations, network security issues, and network connection policies
d. Establish an isolated network for public read-only access to selected computers
e. Maintain accounting information for monitoring, detecting attempted attacks, and allowing backtracking to the source of attacks
f. Support incident response and administrative or legal enforcement efforts
g. Establish controls to ensure that only authorized individuals have access to NASA network support resources
h. Assess security implications before allowing connections to the networks or changing network configurations
i. Document the importance, value, and criticality of systems by subnets or segments. Each node will comply with all of the security for the network or network segments to which it connects. Additionally, network connections for nodes supporting BRT information category applications and data shall be isolated from other network nodes security perimeters (such as a firewall) to ensure that the proper level of network isolation is provided
j. Establish an approval process for users, vendors, and contractor organizations wishing to connect to the NASA Center's networks:
   - Obtain Langley RSA tokens for access to the Langley VPN for remote access to Langley NTTS computers

- Notify the Langley IT Security Manager immediately upon discovery of a missing RSA token.
- Notify the Langley IT Security Manager by the close of business of the termination of any employee with a VPN account and return the RSA token to the Langley IT Security Manager within seven days.[1]

k. Develop, implement, and test a Network Emergency Response Plan that will ensure a timely response to network emergencies.
l. Ensure that line managers of nodes understand that they retain ultimate responsibility for their system's security.

4.3 Network Security Baseline Requirements

A network architecture that includes security for both network components and connected systems shall be established and maintained. The responsible task managers and network administrators shall coordinate security requirements for external nodes with the appropriate NASA Center Network Security staff. NASA Center Network Security processes:

a. Establish a security perimeter between Center networks and networks external to the Center
b. Establish acceptance of externally initiated interactive and file transfer sessions across security perimeters
c. Track connections when they cross the security perimeter
d. Restrict services allowed to cross the perimeter
e. Support public-access read-only information servers, or special boundary systems , and test them to ensure that they do not pose an unacceptable threat to the computers inside the security perimeter
f. Support protected message routing for all Center networks, ensuring that messages on protected networks are not accessible to unauthorized users outside of the security perimeter
g. Establish an approval process for supporting organizations wishing to connect to a Center's networks inside the security perimeter
h. Test networks or network segments within the security perimeter to ensure that they comply with established network security requirements
i. Review external connections to the Center
j. Identify networked nodes with stricter controls in order to provide them with notification of problems such as specific attacks or scheduled outages
k. Establish restrictions and controls to prevent networked nodes from having "back door" connections to untrusted systems . Network nodes cannot be simultaneously connected to a protected network and a nonprotected network. Physical disconnection from all nonprotected networks is required prior to the establishment of a connection to a node on a protected network.

4.4 Network Multi-user System , Server, and Mainframe Requirements

Network multi-user systems, servers, and mainframes have additional security requirements imposed on them solely by operating as a node on a network. This section details the network-related security requirements for nodes by the information category of the system.

[1] If the employee is to be replaced the RSA token can just be disabled until the new employee is in place, otherwise the RSA token shall be returned to the Langley IT Security Manager within seven days.

4.4.1. Authentication Requirements

BRT, SER, and ADM Information Categories

The responsible task manager or network administrator shall implement a process that:

a. Ensures that network devices detect and close broken sessions
b. Prohibits unattended dial-in diagnostics that bypass normal authentication
c. Accepts dial-in connections and connections from public networks only via a boundary system

PUB Information Category

The responsible task manager or network administrator shall implement a process that:

a. Ensures that network devices detect and close broken sessions
b. Disables dial-in diagnostics that bypass normal authentication when they are not in use, or as directed by line management
c. Employs password management features as specified in paragraph 3.3

4.4.2. File Transfer and Remote Logon Protection Requirements

BRT, SER, and ADM Information Categories

The responsible task manager or network administrator shall implement a process that:

a. Prohibits inbound or outbound file transfer from unauthenticated users (i.e., no anonymous file transfer)
b. Restricts access to any privileged network software to a list of specifically authorized users
c. Allows only specifically authorized users to import software
d. Employs digital signatures or multiple checksums to ensure the integrity of file transfer
e. Restricts "proxy " or "trusted " logons
f. Prohibits inbound remote command execution without user authentication

PUB Information Category

The responsible task manager or network administrator shall implement a process that:

a. Allows inbound or outbound file transfer from unauthenticated users only to a restricted set of directories
b. Restricts access to any privileged network software to authorized users
c. Restricts "proxy" or "trusted" logons as specified in paragraph 4.4.1
d. Restricts inbound remote command execution without user authentication

4.4.3. Connection Requirements

BRT, SER, and ADM Information Categories

The responsible task manager or network administrator shall implement a process that:

a. Ensures that the risks associated with connecting to the proposed network/node are acceptable
b. Ensures that "trusted" network partners (e.g., those the local system trusts to authenticate users) have implemented security protections equivalent to or acceptable to the local system

PUB Information Category

The responsible task manager or network administrator shall implement a process that evaluates network connections according to IT security policies, procedures, and guidance

5. PHYSICAL SECURITY REQUIREMENTS

The following physical security provides protect NASA IT resources from human, natural, and accidental damage.

5.1. Entry Control

Entry control is the process by which only authorized individuals are allowed physical access to NASA IT resources. Procedures shall recognize the difference among environments, such as computer rooms, offices, laboratories, and mechanical/electrical equipment rooms. Regardless of the environment, line management is responsible for the data, applications, hardware, and other equipment of which the facility is comprised. The following paragraphs discuss appropriate controls for the different types of NASA IT system processing environments.

5.1.1. Controlled Access Areas

Controlled access areas usually house high-value equipment or equipment that performs mission- or life-critical functions. Only personnel with defined business needs shall be authorized to enter controlled access areas. Authorized personnel shall be issued appropriate badges and/or personal recognition methods to permit entrance. A list of personnel granted ongoing access should be maintained and reconciled at least annually. Personnel who need to enter only occasionally should be escorted or issued temporary badges. A record should be kept of their visits.

5.1.2 Laboratory Areas /Computer Rooms

A laboratory/computer room is defined as a common area where a collection of NASA IT resources is housed and where access mechanisms are not required. A facility manager shall be designated. Several users may share the resources. In this environment, the laboratory manager shall be responsible for implementing appropriate controls and procedures for the entire laboratory.

5.1.3 Office Areas

Each NASA computer resource in an office area shall be assigned to an individual user who is responsible for the resource. This individual shall be responsible for protecting the equipment and information processed by the equipment. Information may be protected in a variety of ways: locking the workstation (if the workstation keys are unique); employing software access controls on the workstation; locking the office housing the workstation; or keeping the information on removable media which are locked in a desk, file cabinet, or safe as necessary when unattended.

5.2 Protection of IT Resources from Fire and Water

Proper fire barriers within, above, and below the operational area plus adequate fire alarm, overhead fire sprinklers, and fire suppression systems shall be in place. Properly positioned, hand-operated extinguishers shall be available. Waterproof covers shall be provided for all appropriate IT resources located in the facility, and adequate floor panel lifters shall be available. Appropriate smoke alarms shall also be installed as well as under-floor water detectors, where applicable.

5.3 Electric Power

The operation of NASA IT equipment depends on the availability of adequate and reliable electric power. The criticality of the data processing functions performed by a facility shall determine the degree of power reliability required. Because the loss of electrical power may result in an immediate cessation of equipment operations, a thorough analysis of potential points

of utility failure and available backup measures (i.e., installation of an uninterruptible power supply) shall be conducted. Special attention shall be given to emergency shutdown controls within a facility. In case of a power failure, emergency (i.e., battery-powered) lights shall be installed and procedures in place to periodically check their operation.

In major NASA IT facilities, a prominently labeled master control switch(es) shall be located at each principal exit from the electronic equipment area. These switches shall disconnect power to all electronic equipment and are in addition to any emergency shutdown for individual machines or other units of equipment. Switches shall be provided at egress points from the electronic equipment area to permit the shutdown of air handling equipment. Manually activated exhaust and ventilating systems shall have startup and shutdown switches at the egress points.

5.4 Facility Housekeeping

Facility housekeeping plays an important part in implementing a sound physical security program. Food or beverages shall not be allowed in facilities. Combustible supplies of cleaners, paper boxes, and cards shall be in equipment areas only as needed. In accordance with safety regulations, approved storage areas shall be provided external to the facility for large numbers of combustible items.

5.5 IT Resource Protection

NASA IT resources include storage media as well as hardware and software. Magnetic media and their data shall be protected against fire, erasure, or inadvertent/malicious damage by humans.

All media of value shall be handled with care and stored in protected areas with adequate accounting procedures and environmental controls. Media containing backups shall be stored in a separate facility.